

**REMARKS/ARGUMENTS**

Claims 1-15 and 18-30 are pending in the present application, of which claims 1 and 18 are independent. Claims 1-15, 18, and 23-30 are hereby amended. No new matter has been added.

The courtesies extended to Applicant's representatives by Examiner of Record Trong Nguyen and Supervisory Patent Examiner Nasser Moazzami during the interview held on June 11, 2009, are appreciated. The reasons presented at the interview as warranting favorable action are incorporated into the remarks below and constitute Applicant's record of the interview.

Entry of this Amendment is proper under 37 CFR § 1.116 since the amendments: place the application in condition for allowance (for the reasons discussed herein); do not raise any new issues requiring further search and/or consideration (because the amendments amplify issues previously discussed throughout the prosecution); satisfy a requirement of form asserted in the previous Office Action; do not present any additional claims; and place the application in better form for appeal, should an appeal be necessary.

**OBJECTIONS TO THE CLAIMS**

On page 3-6, the Office Action objects to claims 1-15, 18, and 23-30. Applicant respectfully traverses these objections.

On page 3, the Office Action alleges “a fourth variable  $Br_2$ ” on line 11 of claim 1 is ambiguous. On page 4, the Office Action alleges that “a fourth variable  $Br_2$ ” on line 16 of claim 18 is ambiguous. In both cases, Applicant replaces “a fourth variable  $Br_2$ ” with -- B multiplied by a fourth variable  $r_2$  --.

In addition, as discussed during the interview on June 12, 2009, Applicant hereby adds “using the modulus in the cryptographic calculation” to both independent claims. As suggested by the Examiner, this subject matter recites the cryptographic calculation of the preambles in the body of the claims. This subject matter finds support, for example, in paragraph [0015] of the specification.

On page 3, the Office Action objects to the recitation of “a method according to” on line 1 of claims 2-13. In response, Applicant changes this language to -- the method of -- to avoid use of the indefinite article “a.”

On page 3, the Office Action alleges that “repeating the combined multiplication operations and reduction operation” on line 2 of claim 4 lacks an antecedent. In response, Applicant replaces this language with -- repeating the effecting step of claim 3 --.

On page 3, the Office Action alleges that the recitation of “wherein, when a last multiplication gives an overflow, the overflow is added to a part of a selected number” on line 2 of claims 6 and 7 is ambiguous. A similar objection on page 5 refers to line 3 of claims 23 and 24. In response, Applicant hereby eliminates the

use of “when” by replacing this language with positive statements in both locations:  
-- adding an overflow from a last multiplication -- and -- adding the first variable  $n_0$  to the overflow --.

On page 4, the Office Action alleges that “the next multiplication” on line 3 of claim 8 lacks an antecedent. On page 5, the Office Action alleges that “the next multiplication” on line 4 of claim 25 lacks an antecedent. In response, Applicant replaces “the next multiplication” with -- a subsequent multiplication --.

On page 4, the Office Action alleges that “the number” on line 2 of claim 9 lacks an antecedent. On page 5, the Office Action alleges that “the number” on line 2 of claim 26 lacks an antecedent. In response, Applicant changes “the number” to - a number -- to avoid use of the definite article “the.”

On page 4, the Office Action alleges that the recitation of “when” on line 3 of claim 10 is ambiguous and that “the number” on line 3 of claim 10 lacks an antecedent. On page 5, the Office Action alleges that the recitation of “when” on line 3 of claim 27 is ambiguous and that “the number” on line 3 of claim 27 lacks an antecedent. In response, Applicant deletes this clause in both locations.

On page 4, the Office Action alleges that the recitation of “when” on line 4 of claims 14 and 15 is ambiguous. In response, Applicant deletes this clause.

On page 4, the Office Action alleges that "modulus performs" should be amended to -- modulus and performs -- on line 11 of claim 18. In response, Applicant adopts the Examiner's suggestion.

On page 5, the Office Action alleges that "the" should be added before "apparatus" on line 1 of claim 26. In response, Applicant adopts the Examiner's suggestion.

On pages 5 and 6, the Office Action alleges that line 3 of claims 28-30 is unclear. In response, Applicant deletes this material.

For the reasons listed above, Applicant respectfully requests withdrawal of all of the claim objections.

#### **REJECTIONS UNDER 35 U.S.C. § 103**

On pages 6-15, the Office Action rejects claims 1-5, 14, 15, and 18-22 under 35 U.S.C. § 103(a) as allegedly unpatentable over U.S. Patent No. 6,366,673 to Hollmann (hereinafter "Hollmann") in view of U.S. Patent Application No. 2002/0059353 to Koc (hereinafter "Koc"). On pages 15-17, the Office Action rejects claims 6, 7, 23, and 24 under 35 U.S.C. § 103(a) as allegedly unpatentable over Hollmann in view of Koc, further in view of U.S. Patent Application No. 2002/0010730 to Blaker (hereinafter "Blaker"). On pages 17-20, the Office Action rejects claims 8-10 and 25-27 under 35 U.S.C. § 103(a) as allegedly unpatentable

over Hollmann in view of Koc, further in view of U.S. Patent No. 6,240,436 to McGregor (hereinafter "McGregor"). On pages 21-26, the Office Action rejects claims 11-13 and 28-30 under 35 U.S.C. § 103(a) as allegedly unpatentable over Hollmann in view of Koc, further in view of the article to Lenstra et al (hereinafter "Lenstra"). Applicant respectfully traverses these rejections.

All of these rejections rely upon the newly cited Koc reference. As correctly conceded on page 7 of the Office Action, Hollmann does not provide the recited steps of multiplying, dividing, and adding. The Office Action then attempts to remedy this admitted deficiency by applying Koc's teachings. However, as agreed during the interview of June 12, 2009, Koc clearly fails to disclose, suggest, or teach the recited subject matter. In particular, Koc's "Montgomery" system resembles the conventional calculation method described in paragraphs [0008-0010] of the published version of the current specification.

Applicant respectfully submits that Blaker, McGregor, and Lenstra fail to remedy the deficiencies of Hollman described above for independent claims 1 and 18. Claims 2-15 depend from independent claim 1. Claims 19-30 depend from independent claim 18. Thus, Applicant respectfully submits that claims 2-15 and 19-30 are allowable at least on the basis of their respective dependencies from allowable claims. Accordingly, Applicant respectfully requests withdrawal of the rejection of claims 1-15 and 18-30 under 35 U.S.C. § 103(a).

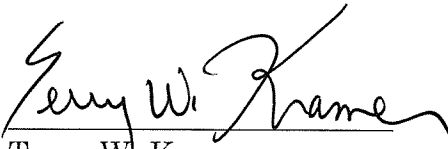
**CONCLUSION**

In view of the remarks above, Applicant believes that each of the rejections/objections has been overcome and the application is in condition for allowance. Should there be any remaining issues that could be readily addressed over the telephone, the Examiner is asked to contact the attorney overseeing the application file, David Cordeiro, of NXP Corporation at (914) 860-4296.

In the event that the fees submitted prove to be insufficient in connection with the filing of this paper, please charge our Deposit Account Number 50-0578 and please credit any excess fees to such Deposit Account.

Respectfully submitted,  
**KRAMER & AMADO, P.C.**

Date: June 18, 2009

  
Terry W. Kramer  
Registration No.: 41,541

Please direct all correspondence to:  
Corporate Patent Counsel  
NXP Intellectual Property & Standards  
1109 McKay Drive; Mail Stop SJ41  
San Jose, CA 95131  
CUSTOMER NO.: 65913